HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,472	04/23/2001	John J. Bowe	Zolera/Patent	5737

21034 7590 06/21/2005

IPSOLON LLP
805 SW BROADWAY, #2740
PORTLAND, OR 97205

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/840,472	**Applicant(s)** BOWE ET AL.	
	Examiner Benjamin E Lanier	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33,56-82 and 91-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33,56-82,91-104* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 April 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. The amendment filed 16 May 2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: authenticating for a first client a data object that is provided by a second client. The specification does not disclose such a method of indirect authentication, but rather discloses that a client requests authentication of data and receives the results without the use of the second client.

Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

2. Applicant's arguments filed 16 May 2005 have been fully considered but they are not persuasive. Applicant's arguments that the prior art does not disclose allowing the server to function as an authenticating intermediary for a data object passed between the first and second clients is not persuasive because Pfitzmann discloses the use of Group-Oriented Signature Schemes that allow for many users within a group to authenticate specific signers within their group using the server (Pages 30-31).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-33, 56-59, 61-82, 93-104 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The added material which is not supported by the original disclosure is as follows: authenticating for a first client a data object that is provided by a second client. The specification does not disclose such a method of indirect authentication, but rather discloses that a client requests authentication of data and receives the results without the use of the second client.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 17, 18, 56, 58, 59, 61, 62, 65, 67, 91, 104 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 17, 56, 58, 59, 61, 62, 65, 67, 104, recite the limitation of "a signing client", which renders the claim vague and indefinite because the actual signature is generated at the digital signature server. It is therefore unclear exactly to what the "signing client" is referring.

8. Claims 91, 104, recite the limitation of "a verifying client", which renders the claim vague and indefinite because the actual signature is verified at the digital signature server. It is therefore unclear exactly to what the "verifying client" is referring.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. Claims 1-5, 8-19, 22-31, 33, 56-68, 70-80, 91-99, 102-104 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, U.S. Patent No. 6,490,682, in view of Pfitzmann. Referring to claims 1, 2, 11-19, 22-31, 33, 56, 57, 59, 60, 62-68, 71-80, 91-95, 102-104, Vanstone discloses a log-on verification protocol wherein a client generates a random number that is transmitted along with a data request to a server (Col. 3, lines 15-18), which meets the limitation of receiving a data object transmitted from the client to the server via the communications channel, the additional data is obtained from a device, the device receives the data object prior to subsequent processing by the server. The server then computes a hash on the concatenation of requested data and the random number (Col. 3, lines 18-20), which meets the limitation of the property fields further comprise additional data that is signed by a key private to the server, the additional data is derived by processing the data object using a pre-determined hash function, transform function. The server then computes a signature on the hash using the

private key of the client (Col. 3, lines 20-22), which meets the limitation of generating a signature by processing the data object, associating the signature with the data object to create a signed object, creating and managing private keys to use in the step of generating the signature, the server assigns a private key to the client. Both the applet and the signature are then sent to the client (Col. 3, lines 22-23). Vanstone discloses that the client verifies the validity of the signature, and not the server. Pfitzmann discloses a digital signature verification scheme that uses server aided generation and verification (Page 29), which meets the limitation of authenticating the signed object, subsequently upon request, deriving from the singed object information representative of the data object and the signature, generating a comparison value using the information representative of the data object, determining whether the comparison value and at least a portion of the signature meet a predetermined criteria, property field further comprises key information used to generate the comparison value. It would have been obvious to one of ordinary skill in the art at the time the invention was made to verify the digital signature at the server where the signature was created because the system of Vanstone uses hardware tokens such as smartcards (Col. 2, line 25) and Pfitzmann discloses that using server-aided signing and verification is beneficial to systems utilizing smartcards in order to conserve computing power by delegating some of their computations to the server (Pfitzmann, Page 29). Pfitzmann further discloses the use of Group-Oriented Signature Schemes that allow for many users within a group to authenticate specific signers within their group using the server (Pages 30-31), which would meet the newly added limitations that amount to allowing a server to function as an authenticating intermediary for a data object passed between the first and second clients. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the verification protocol of Vanstone to support Group-Oriented Signature Schemes so that group members can authenticate signatures from other group members as taught by Pfitzmann (Page 31).

Referring to claims 3, 4, 58, 61, 96, Vanstone discloses that the server can authenticate the client using the client ID (Col. 2, lines 33-45), which meets the limitation of the client is authenticated by the server using information representative of the client.

Referring to claims 5, 97-99, Vanstone discloses that the client authentication utilizes a PIN (Col. 2, lines 26-27), which meets the limitation of the information representative of the client comprises a password provided by the client.

Referring to claims 8-10, Vanstone discloses the use of public key certificate authentication (Col. 2, lines 47-51), which meets the limitation of public key based processing step includes the presentment of a client certificate.

Referring to claim 70, Vanstone discloses that the client ID is used as an index in the server to find the associated private key (Col. 2, lines 34-39).

12. Claims 6, 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, U.S. Patent No. 6,490,682, in view of Pfitzmann as applied to claims 1, 3 above, and further in view of Pavlik, U.S. Patent No. 6,807,633. Referring to claims 6, 7, Vanstone discloses a log-on verification protocol wherein a client generates a random number that is transmitted along with a data request to a server (Col. 3, lines 15-18), which meets the limitation of receiving a data object transmitted from the client to the server via the communications channel. The server then computes a hash on the concatenation of requested data and the random number (Col. 3, lines 18-20). The server then computes a signature on the hash using the private key of the client (Col. 3,

lines 20-22), which meets the limitation of generating a signature by processing the data object, associating the signature with the data object to create a signed object. Both the applet and the signature are then sent to the client (Col. 3, lines 22-23). Vanstone discloses that the client verifies the validity of the signature, and not the server. Pfitzmann discloses a digital signature verification scheme that uses server aided generation and verification (Page 29), which meets the limitation of authenticating the signed object, subsequently upon request, deriving from the singed object information representative of the data object and the signature, generating a comparison value using the information representative of the data object, determining whether the comparison value and at least a portion of the signature meet a predetermined criteria. Vanstone and Pfitzmann fail to disclose using a secure channel such as SSL for client authentication. Pavlik discloses a digital signature system where a client is authenticated over a network by way.of a SSL secure channel (Col. 6, lines 37-49). It would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate the client of Vanstone over an SSL secure channel so as to provide a digital signature system with electronic documentation, such as credit card information and/or bank account information as taught in Pavlik (Col. 6, lines 50-53).

13. Claims 20, 21, 32, 69, 81, 82, 100 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, U.S. Patent No. 6,490,682, in view of Pfitzmann as applied to claims 17-20 above, and further in view of Epstein, U.S. Patent No. 6,601,172. Referring to claims 20, 32, 32, 69, 81, 82, 100, Vanstone discloses a log-on verification protocol wherein a client generates a random number that is transmitted along with a data request to a server (Col. 3, lines 15-18), which meets the limitation of receiving a data object transmitted from the client to

the server via the communications channel. The server then computes a hash on the concatenation of requested data and the random number (Col. 3, lines 18-20). The server then computes a signature on the hash using the private key of the client (Col. 3, lines 20-22), which meets the limitation of generating a signature by processing the data object, associating the signature with the data object to create a signed object. Both the applet and the signature are then sent to the client (Col. 3, lines 22-23). Vanstone discloses that the client verifies the validity of the signature, and not the server. Pfitzmann discloses a digital signature verification scheme that uses server aided generation and verification (Page 29), which meets the limitation of authenticating the signed object, subsequently upon request, deriving from the singed object information representative of the data object and the signature, generating a comparison value using the information representative of the data object, determining whether the comparison value and at least a portion of the signature meet a predetermined criteria. Vanstone and Pfitzmann fail to disclose the signed object containing a timestamp. Epstein discloses a digital signature transmission system wherein the signed documents contain a digital signature (Abstract & Col. 1, lines 11-18). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the server of Vanstone to timestamp the signed object in order to prove that no one has altered or revised the digital document since a certain date such as the alleged creation date or transmittal data of the document as taught by Epstein (Col. 1, lines 14-16).

Referring to claim 21, Vanstone discloses that the client ID is used as an index in the server to find the associated private key (Col. 2, lines 34-39).

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

Gilberto B
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100